Zone Editor

(*cPanel >> Home >> Domains >> Zone Editor*)

In This Document

Related Documentation

- Email Routing
- Zone Editor
- Track DNS

For Hosting Providers

- DNS
- How to List Domains with DNSSEC
- How to Rotate a DNSSEC Key
- How to Use cPanel's PowerDNS
- How to Use MyDNS-NG

Overview

DNS (Domain Name Service) converts human-readable domain names (for example, `example.com`) to computer-readable IP addresses (for example, `192.0.32.10`). DNS relies on zone records that exist on your server to map domain names to IP addresses.

Several different types of records reside in a domain's zone file. This feature allows you to create, edit, and delete the following records:

- A
- AAAA
- CAA (Certificate Authority Authorization Record)
- CNAME (Canonical Name Record)
- DMARC (Domain-based Message Authentication, Reporting, and Conformance)
- MX (Mail Exchanger)
- SRV (Service Record)
- TXT (Text Record)

⚠ **Note:**

To access all available zone record types and records that the system automatically generated , your systems administrator **must** enable the following features in WHM's *Feature Manager* interface (*WHM >> Home >> Packages >> Feature Manager*):

- *Zone Editor (A, CNAME)*
- *Zone Editor (AAAA, CAA, SRV, TXT)*

Domains

This interface displays your account's domains. For each domain in the list, you can perform some actions directly. Click the text to perform that action.

Text	Action
A Record	Add an A record for this domain.
CNAME Record	Add a CNAME record for this domain.
MX Record	Add an MX record for this domain.
DNSSEC Record	Enable or disable DNSSEC for this domain.
Manage	Add or edit additional records for this domain.

To refresh the list of domains, click the gear icon (⚙) and select *Refresh List.*

Manage Zone

This interface displays the zone records for the selected domain. To filter the list of zone records, enter a name in the text box or select one of the record type filters.

Add a record

To add a record, perform the following steps:

1. Click *Manage* next to the domain that you wish to modify.
2. Click the arrow next to *Add Record* to select a record type:
    - *Add A Record* — This record maps hostnames to IP addresses. A records allow DNS servers to identify and locate your website and its various services on the Internet. Without appropriate A records, your visitors cannot access your website, FTP site, or email accounts.

> ⚠ **Note:**
>
> The system configures your DNS records so that visitors can resolve your website and its services, such as FTP and email. **Only** add A records when you add a service that cPanel & WHM or your service provider does not provide.

- *Add AAAA Record* — This record maps hostnames to IPv6 addresses.
- *Add CAA Record* — This record allows you to specify which certificate authority (CA) will issue an SSL certificate for a domain.

Element	Description	Possible values
Flag	Whether the CA will issue an SSL certificate if the CAA Resource Record contains unknown property tags. For more information about CAA record flags, read the RFC 6844 Documentation.	• *0* — Non-critical. The CA will issue an SSL certificate if the CAA Resource Record contains unknown property tags. • *1* — Critical. The CA will **not** issue an SSL certificate if the CAA Resource Record contains unknown property tags.
Tag	The CAA record's property type.	• *issue* — Authorize a CA to issue a certificate for the domain. • *issuewild* — Authorize a CA to issue a wildcard certificate for the domain. • *iodef* — Specify a URL to which a CA may report policy violations.
Value	The CA's domain, or the CA's URL if you select the *iodef* element.	• A valid SSL provider. • A mailto URL or a standard URL.

If no CAA records exist for a domain, all CAs can issue certificates for that domain. If conflicting CAA records already exist, remove the existing CAA records or add one for the desired CA.

For example, a CAA record for Sectigo® would resemble the following example, where `example.com` represents the domain name:

```
example.com. 86400 IN CAA 0 issue "sectigoca.com"
```

For more information about a CA's requirements, read their documentation.

- *Add CNAME Record* — This record creates an alias for another domain name, which DNS looks up. This is useful, for example, if you point multiple CNAME records to a single A record in order to simplify DNS maintenance.

> ⚠ **Note:**
>
> You **cannot** point a CNAME record at an IP address.

- *Add DMARC Record* — This record indicates the action for a mail server to take when it receives mail from this domain, but that message fails SPF and DKIM checks. If you select this option, the system creates a TXT record with a default DMARC record. The system also displays a form that allows you to specify the domain's DMARC policy (*None, Quarantine,* or *Reject*), as well as the following optional parameters:

> ⚠ **Note:**
>
> If you do not specify a valid parameter, the system will **not** save the parameter when you create the record.

Option	Description	Possible values
Subdomain Policy	The action that the recipient's mail server should perform when it receives mail from a subdomain of this domain, but that message fails SPF and DKIM checks.	• *None* — Do **not** perform any action for spam email messages. • *Quarantine* — Send spam email messages to a different folder on the account. • *Reject* — Reject spam email messages.

DKIM Mode	The Domain Keys Identified Mail (DKIM) level that the system will enforce for the domain.	- *Relaxed* — The system allows some email messages from domains that it does not recognize. - *Strict* — The system rejects **all** email messages from domains that it does not recognize.
SPF Mode	The Sender Policy Framework (SPF) level that the system will enforce for the domain.	- *Relaxed* — The system allows some email messages from senders that it does not recognize. - *Strict* — The system rejects **all** email messages from senders that it does not recognize.
Percentage	The percentage of email messages that you wish for the system to filter. **Note:** This parameter's value defaults to *100*.	An integer value between *0* and *100*.
Generate Failure Reports When	The error reporting policy between the sender and receiver's Mail Transfer Agents.	- *Any checks fail* — Send a report to both the sender and receiver if **any** email checks fail. - *All checks fail* — **Only** send a report to both the sender and receiver if all of the email checks fail.
Report Format	The format that the system uses to report an email message's possible spam status.	- *AFRF* — Authentication Failure Reporting Format. - *IODEF* — Incident Object Description Exchange Format.
Report Interval	The amount of time, in seconds, that elapse between each aggregate email message report. **Notes:** - This parameter's value defaults to *86400*. - This value does **not** include email failure messages.	A positive integer.
Send Aggregate Mail Reports To	A comma-delimited list of URIs to which to send aggregate email message reports. To add a size limit for the report, affix an exclamation point, a number, and a file size multiplier to the end of the URI. You can specify the following size multipliers: - `k` — Kilobytes. - `m` — Megabytes. - `g` — Gigabytes. - `t` — Terabytes. **Note:** If your URI includes a comma, you **must** URI-encode the comma.	`mailto:reports@example.com!50m`
Send Failure Reports To	A comma-delimited list of URIs to which to send failure email message reports.	`mailto:reports@example.com!50m`

- *Add MX Record* — This record allows you to route a domain's incoming mail to a specific server. Changes that you make to a domain's MX (Mail Exchanger) control where the system delivers email for a domain.
- *Add SRV Record* — This record provides information about available services on specific ports on your server.

Note:

The SRV record **must** point at a hostname with an A (or AAAA) record. You **cannot** point an SRV record at a CNAME record.

Option	Description	Possible values
Priority	The service record's priority value.	A positive integer that represents the target host's priority order.
Weight	The system uses this value to rank entries with the same `priority` value.	A positive integer that represents the target host's weight against other hosts with the same *Priority* value.
Port	The target host's port.	A positive integer that represents a port number. **Note:** For a complete list of ports, read our How to Configure Your Firewall for cPanel Services documentation.
Target	The service's target host.	A valid hostname.

- *Add TXT Record* — This record contains text information for various services to read. For example, TXT records can specify data for the SPF, DKIM, or DMARC email authentication systems.
  Click the links below to view examples of each TXT record:

  Note:

  The TXT record text box accepts invalid data and does **not** issue a warning.

  v=spf1 +a +mx +ip4:10.215.218.151 ~all

  v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA14CK7pzW3Q4NHyJv/NIUG2vxuW8cDLnrQyjnpf0XQCHkFMnBdampzVG/T15U4P7W3YKImR6aF+QhM6WRZdXaOQqdkkkGc+VdYnH415ZikqSvfwSQ+n2fdIEVHvOkLyl/qSQkNhijtz48qb874keiYimo9Gsdg7mlhURImqPlL9zsGFcBpogmW00bnwmeiyeFbBY+d0QJRAelECpIbdWQfiCq1tUMm1pMGI5GHmnJVs3ToPvRoH2J4SQpOO91smkwaQPEEdLVXTMpLuKcvOOjotwzeVX5A4RBfuAaKjk7z0xdkTnsDivFJSqqNBLtT0v8cv6JjDgWZ8pYKBC65mdWxwIDAQAB;

  v=DMARC1;p=none;rua=mailto:user@example.com

  Note:

  On servers that run CentOS 7, you may see a `named` warning about the absence of SPF resource records on DNS.

  - This warning is **not** relevant on CentOS 7 servers, because RFC 7208 deprecated SPF records. CentOS 7 servers use TXT records instead of SPF records.
  - Red Hat 7.1 and CentOS 7.1 both contain `bind-9.9.4-23.el7`, which is an updated version of BIND that complies with RFC 7208. To resolve this issue, update your operating system to a version that contains the updated version of BIND. For more information, read the Red Hat Bugzilla case about SPF record errors.

2. Enter the appropriate information for the record type that you selected.
3. Click *Add Record*.

Note:

Use cPanel's *Email Deliverability in cPanel* interface *(cPanel >> Home >> Email >> Authentication)* to manage SPF and DKIM records.

Edit a record

To edit a record, perform the following steps:

1. Click *Manage* next to the domain you want to modify.
2. Click *Edit* next to the record that you wish to edit.
3. Change the information in the text boxes as necessary.
4. Click *Edit Record* to save your changes, or click *Cancel* to discard them.

Delete a record

To delete a record, perform the following steps:

1. Click *Manage* next to the domain you want to modify.
2. Click *Delete* next to the record that you wish to remove.
3. Click *Delete* i n the confirmation dialog box.

Reset zone files

Important:

- This feature erases **any** modifications that you made to your zone records. The system attempts to save the domain's TXT entries. We recommend that you record any changes that you wish to save before you use this feature.
- To reset your DNS zone files, your systems administrator **must** enable the following features in WHM's *Feature Manager* interface (*WHM >> Home >> Packages >> Feature Manager*):
    - *Zone Editor (A, CNAME)*
    - *Zone Editor (AAAA, CAA, SRV, TXT)*

To reset your DNS zone files to the defaults that your hosting provider specifies, perform the following steps:

1. If this account owns more than one domain, click *Manage* next to the domain that you wish to reset.
2. Click the gear icon (⚙) and select *Reset Zone*.
3. Read the warning about the consequences.
4. Click *Continue* to reset your zone, or *Cancel* to return to the *Manage Zone* interface.

DNSSEC

Important:

This feature **only** appears if your system administrator disables DNS clustering **and** installs PowerDNS in WHM's *Nameserver Selection* interface (*WHM >> Home >> Service Configuration >> Nameserver Selection*).

DNS Security Extensions (DNSSEC) add a layer of security to your domains' DNS records. DNSSEC uses digital signatures and cryptographic keys to authenticate DNS responses. These digital signatures protect clients from various forms of attack, such as Spoofing or a Man-in-the-Middle attack.

Important:

- DNSSEC keys remain on a server after you terminate an account. If you restore an account on the same server from which you deleted it, the account’s DNSSEC keys remain valid.
- If you transfer the account to another server, you **must** reconfigure DNSSEC for the domains and update the domain server records on the registrar. The system does **not** include DNSSEC keys in an account’s backup file.

To transfer an account with DNSSEC enabled domains, perform the following steps for each domain:

1. Remove the Domain Server (DS) records from the registrar.
2. Wait for the changes to propagate (This may take up to 72 hours).
3. Disable DNSSEC on the domain (optional).
4. Transfer the account to the new server.
5. Enable DNSSEC on the new server.

If you do not remove the old DS records from the registrar, the domains may produce DNS resolution issues due to invalid DNSSEC responses.

Enable DNSSEC

To enable DNSSEC for a domain, perform the following steps:

1. If this account owns more than one domain, click *DNSSEC* next to the domain you want to modify.
2. Click *Enable.* The system will generate a new DNSSEC key, and a new line will appear that contains the following information:

Column	Description
Key Tag	An integer value that identifies the domain's DNSSEC record.
Algorithm	The record's encrypted signature.
Digest Type	The algorithm type that constructs the digest. Select the digest type that your registrar supports.
Digest	An alpha-numeric string that the algorithm generates.

Important:

After you generate the domain's DNSSEC key, you **must** configure a Domain Server (DS) record with your domain registrar. Click the links below for DS record instructions with some of the most popular domain registrars.

To configure a DS record with GoDaddy, perform the following steps:

1. Click *Manage.*
2. In the upper-right corner of the interface, select the *list* view.
3. Select the domain for which to create a DS record.
4. In the *DS Records* section of the *Settings* interface, click *Manage.*
5. Click *Add DS Record*.
6. Enter the DNSSEC key's information in the text boxes and click *Next*. The system will validate the DS record information that you added.
7. Click *Next,* and then click *OK.*

To configure a DS record with NameCheap, perform the following steps:

1. Click *Domain List* in the left menu*.*
2. Select the domain for which to configure a DS record and click *Manage*.
3. Click *Advanced DNS.*
4. Move the *DNSSEC* toggle button to *on*. The DS records menu will appear.
5. Click *ADD NEW DS.*
6. Enter the DNSSEC key's information in the text boxes.
7. Click *SAVE ALL CHANGES.*

To configure a DS record with OpenSRS, perform the following steps:

1. Click *Domains*.
2. Locate the domain for which to configure a DS record and click the domain's name.
3. Scroll down to the *DNSSEC* section and click *Edit*. The DS records menu will appear.
4. Enter the DNSSEC key's information in the text boxes.
5. Click *Save.*

Disable DNSSEC

To disable DNSSEC for a domain, perform the following steps:

1. If this account owns more than one domain, click *DNSSEC* next to the domain you want to modify.
2. Click *Disable.*

Important:

After you disable DNSSEC, you **must** delete the DS record with your domain registrar. Click the links below for DS record instructions with some of the most popular domain registrars.

To delete a DS record with GoDaddy, perform the following steps:

1. Click *Manage.*
2. In the upper-right corner of the interface, select the *list* view.
3. Select the domain for which to delete a DS record.
4. In the *DS Records* section of the *Settings* interface, click *Manage.*
5. Locate the DS record that you wish to delete and click *Remove*. The system will validate the DS record information that you removed.
6. Click *Next.*
7. Click *OK.*

To delete a DS record with NameCheap, perform the following steps:

1. Click *Domain List* in the left menu*.*
2. Select the domain for which to delete a DS record and click *Manage*.
3. Click *Advanced DNS.*
4. Click the in the DS record's row to delete the record.
5. Click *SAVE ALL CHANGES.*
6. Move the *DNSSEC* toggle button to *Off.*

To delete a DS record with OpenSRS, perform the following steps:

1. Click *Domains*.
2. Locate the domain for which to delete a DS record and click the domain's name.
3. Scroll down to the *DNSSEC* section and click the next to the *Key Tag* text box.
4. Click *Save.*